LËTZEBUERGER Journal

La cyberpandémie

Par Misch Pautsch, Lex Kleren

Publié le 02 déc. 2021

Changer en allemand pour l'article original

Écouter cet article

11:03

Le nombre d'attaques informatiques contre des hôpitaux a considérablement augmenté dans le monde au cours des deux dernières années, avec des conséquences parfois mortelles. Les hôpitaux luxembourgeois ont réussi à repousser les attaques. Mais la lutte contre les bandes organisées, souvent soutenues par un État, se poursuit. La pression monte.

Dans les coulisses des scènes dramatiques qui se déroulent déjà dans les hôpitaux, une deuxième bataille, invisible, se déroule chaque jour : des groupes organisés de *crackers* profitent de la pandémie pour intensifier leurs attaques contre le secteur de la santé. Avant la pandémie, les attaques de *ransomware*, au cours desquelles les utilisateur·rice·s se voient bloquer l'accès à leur ordinateur infecté jusqu'à ce qu'ils·elles versent une rançon – les ordinateurs infectés affichent un écran d'aide « pratique » énumérant les étapes à suivre pour les débloquer –, étaient programmées pour toucher sans but précis le plus grand nombre de personnes possible : plus il y avait de victimes, plus il y avait de rançons. Entre-temps, le focus semble s'être déplacé, explique Paul Rhein, directeur de l'équipe gouvernementale Computer Emergency Response Team (GOVCERT.lu), qui dépend du Haut Commissariat à la sécurité nationale : « Le grand changement au cours des dernières années est que le focus est passé des particuliers aux entreprises ».

Quand les viruses informatiques sont mortels

Les attaques de *ransomware* à grande échelle ne se limitent pas au secteur de la santé, comme l'ont montré les attaques contre le plus grand *pipeline* d'essence des États-Unis, le pipeline Colonial, ou les usines de transformation de viande de JBS, le plus grand groupe de transformation de viande au monde. Lors de ces « campagnes »,

des ordinateurs ont été bloqués de manière coordonnée aux États-Unis, au Canada et en Australie, les deux fois avec des conséquences dévastatrices pour des chaînes d'approvisionnement étendues. « Les hôpitaux constituent, surtout maintenant, dans la situation actuelle, une cible privilégiée pour les cyberattaques », explique M. Rhein. Dans les hôpitaux fortement sollicités, même de petites pannes peuvent entraîner de graves dommages humains. Les responsables sont d'autant plus incité·e·s à payer la rançon réclamée – après tout, des vies humaines sont en jeu.

Au moins un décès à Düsseldorf montre que ces craintes ne sont pas infondées. Ici, une femme a dû être transférée dans un autre hôpital après qu'un *ransomware* a paralysé 30 serveurs de l'hôpital. Le groupe d'inconnu·e·s à l'origine de l'attaque a été inculpé d'homicide. Même si des enquêtes ultérieures ont démontré que la femme n'aurait probablement pas survécu même en absence de cyberattaque, ce cas illustre clairement les risques de telles attaques pour les hôpitaux comme pour leurs patients. Si certains groupes avaient annoncé une « pause Covid » au début de la pandémie, il semble que la situation ait changé. « Ces attaques ont un coût élevé sur tous les fronts », écrit l'Institut CyberPeace de Genève : « Les ressources destinées à la lutte contre le Covid-19 sont paralysées, la sécurité des patients est compromise, des données sensibles sont volées et la confiance de la société dans le système de santé est ébranlée ».

« Malheureusement », regrette M. Rhein, « les auteurs derrière de telles attaques ne sont que rarement amenés à rendre des comptes ». Pour les *crackers*, de telles attaques sont associées à un faible risque et à un profit potentiel très élevé : les demandes de rançon se chiffrent souvent en millions et les enquêtes hors l'UE sont extrêmement difficiles.

Le nombre de cyberattaques contre les hôpitaux a considérablement augmenté depuis le début de la pandémie de Covid-19. Rien qu'entre novembre 2020 et février 2021, le nombre d'attaques contre le secteur de la santé par le biais de différentes cyberattaques telles que « *ransomware, botnets, remote code execution* et attaques *DDoS* », qui endommagent les réseaux, les systèmes ou les ordinateurs de différentes manières, a augmenté de 145% en Europe centrale selon Check Point. Les hôpitaux allemands ont même été touchés par 220% d'attaques supplémentaires. Aux États-Unis, les attaques coordonnées ont obligé certains médecins à prendre des notes manuscrites pendant des jours, les opérations sont devenues impossibles et toute l'organisation et la coordination se sont effondrées pendant des heures, voire des jours. Au Luxembourg aussi, de telles attaques sont devenues plus fréquentes, confirme M. Rhein. « Actuellement, une campagne d'attaque appelée 'Squirrelwaffle' est en cours, qui installe entre autres des *dropers* ou des *trojan* (chevaux de Troie) sur les machines concernées. »

Cette situation pourrait se transformer en une grande campagne de *ransomware*, car les attaques de *ransomware* ne sont que la dernière étape d'attaques coordonnées. Les cyber-attaques se composent généralement de plusieurs étapes répétitives, qui peuvent être plus ou moins élaborées : espionnage, infection, vol de fichiers, et/ou cryptage, chantage et defacement (une attaque sur un site Internet qui modifie son apparence, comparable à du grafitti électronique). Ces attaques se produisent en principe par vagues, qui sont particulièrement marquées lorsque « de nouveaux logiciels ou des logiciels particulièrement performants ont été développés ou adaptés, comme par exemple le logiciel Emotet. De telles attaques ne sont en principe pas limitées à un seul secteur », explique M. Rhein.

« Un réseau de travail pourrait par exemple être infecté en connectant une fois un ordinateur

portable de travail au même réseau qu'un ordinateur portable privé infecté. »

Dennis Fink, Chaos Computer Club Luxembourg

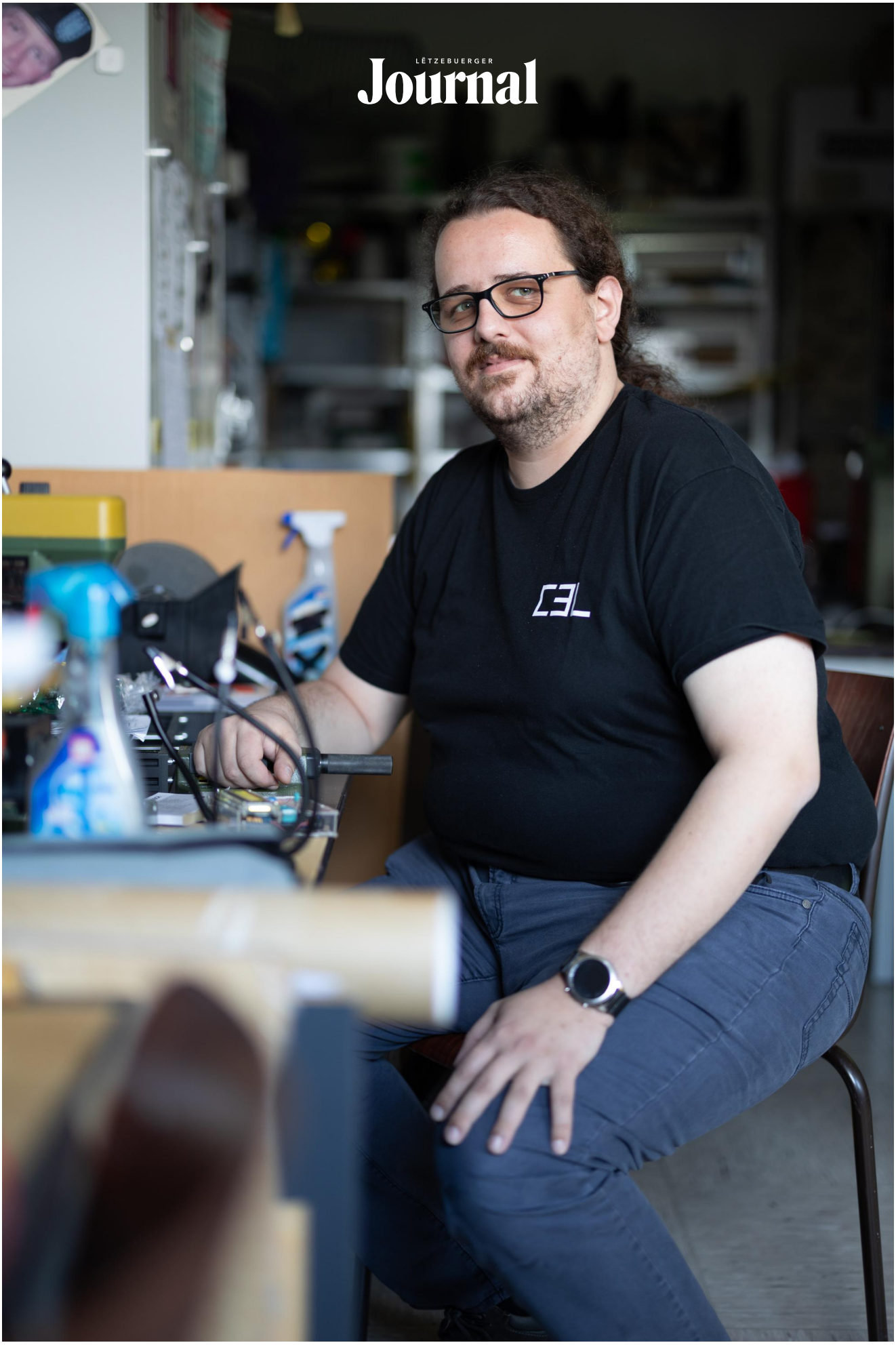
Dennis Fink du Chaos Computer Club Luxembourg (C3L) décrit la perfidie avec laquelle les programmes malveillants peuvent fonctionner à cet égard : « Avec les logiciels malware performants, nous voyons qu'ils font bien plus que de s'installer sur un ordinateur. Un cas survenu dans un hôpital au Royaume-Uni en 2017 a montré comment un logiciel recherchait automatiquement d'autres failles de sécurité sur le réseau à partir d'un appareil infecté. Un réseau de travail pourrait par exemple être infecté en connectant une fois un ordinateur portable de travail au même réseau qu'un ordinateur portable privé infecté ». Une fois que le programme presque invisible s'est propagé dans le réseau, il ouvre la voie à d'autres logiciels, dont les *ransomwares*, qui peuvent ainsi être activés simultanément sur toutes les machines infectées – sans que jamais le·la propriétaire de la première machine touchée ne sache que son ordinateur était le patient zéro.

À cela s'ajoute, comme l'explique M. Fink, le fait que les hôpitaux ont généralement tendance à ne pas mettre immédiatement à jour leurs logiciels – l'une des mesures préventives les plus importantes contre une infection. « Je ne sais pas exactement quelle est la situation au Luxembourg, mais les hôpitaux ont tendance à travailler souvent avec d'anciennes versions de logiciels, car ils préfèrent des systèmes dont ils sont sûrs qu'ils fonctionneront de manière fiable ». Les mises à jour pourraient s'accompagner de problèmes de compatibilité, des bugs inconnus (erreurs de système) pourraient se glisser dans les machines critiques « et ce n'est pas très pratique lorsque le technicien doit mettre à jour manuellement toutes les machines tous les deux jours. Ils préfèrent donc travailler avec d'anciennes versions fiables qui fonctionnent en toute sécurité. Ce n'est pas répréhensible en soi, tant que le système est bien isolé d'internet … ce que je suppose fortement, surtout dans les hôpitaux ».

Arrêt complet

Dans le pire des scénarii, où toute activité doit être arrêtée immédiatement, M. Fink estime qu'en général, « selon le type de logiciel, il n'y a plus grand-chose à faire, à part recourir aux sauvegardes – si elles n'ont pas également été bloquées au moment de

l'attaque – … ou payer. Étonnamment, il semble que dans la plupart des cas, les gens reçoivent effectivement le mot de passe après le transfert d'argent ». Les *crackers* se présentent en tant que « prestataires de services » cordus qui « rendent » leurs données aux gens et veulent en conséquence que leurs « client·e·s » soient satisfait·e·s. Souvent, la fenêtre que l'on ne parvient pas à fermer, énumérant les étapes à suivre pour débloquer l'ordinateur – après l'activation du virus – explique que l'ordinateur a été bloqué « pour protéger les fichiers » parce qu'il a été infecté par un autre programme malveillant. En remerciement de cette « protection », il demande alors à ce que l'on paie la somme indiquée aux bienfaiteur·rice·s inconnu·e·s qui ont « protégé » l'ordinateur. Ironie obscène.



Dennis Fink, Chaos Computer Club Luxembourg

Toutefois, selon le directeur du GOVCERT Paul Rhein, le motif réel derrière les cyberattaques est presque toujours l'argent : « Les tentatives d'extorsion sont généralement motivées par des intérêts financiers. Il n'est bien sûr pas exclu que d'autres aspects jouent un rôle, comme nous l'avons vu dans certaines situations à l'étranger. Mais actuellement, dans notre pays, nous observons toujours qu'il s'agit au final d'extorquer de l'argent. Nous sommes aujourd'hui confrontés à un véritable écosystème dans lequel différents acteurs proposent différents services illégaux pour permettre à d'autres criminels de faire leur métier. »

Selon les expert·e·s, il semble exister un havre de paix pour ces organisations criminelles : la Russie. Car de nombreux « gangs de *ransomware* opèrent depuis l'Ukraine et la Russie selon les experts en cybersécurité » – avec l'approbation silencieuse du Kremlin aux yeux de nombreux analystes – la Russie a été exclue en octobre 2021 d'une réunion de représentant·e·s de 30 pays sur la cybersécurité et les *ransomwares*.

Une manière inhabituelle de se protéger contre les attaques correspondantes étaie de telles accusations, spécule Dennis Fink du C3L : « Si l'on examine le code de beaucoup de ces virus, on constate qu'il existe un critère très précis qui les empêche d'être actifs : les claviers russes. En effet, c'est l'un des principaux critères recherchés par de nombreux virus. Ils semblaient donc exclure très spécifiquement les ordinateurs russophones de leurs campagnes. Probablement dû au fait que les gangs auraient alors plus de problèmes avec l'État que cela n'en vaut la peine. Il faut que je me procure un tel clavier. »

« Les tentatives d'extorsion sont généralement motivées par des intérêts financiers. Nous sommes aujourd'hui confrontés à un écosystème dans lequel les acteurs proposent différents services illégaux pour permettre à d'autres criminels de faire leur métier. »

Paul Rhein, directeur de GOVCERT.lu

Cependant, pour les infrastructures critiques telles que les hôpitaux, installer uniquement des claviers russes ne semble pas être une stratégie prometteuse. La tâche de surveiller ces systèmes importants incombe au GOVCERT, comme l'explique son directeur : « Notre objectif est d'offrir à toutes les organisations relevant de notre compétence la meilleure protection possible contre les cyberattaques, tout en sachant qu'une sécurité à 100% ne peut pas exister. Ce qui a été créé par l'Homme peut aussi être détruit par l'Homme. Mais la dernière et unique infection d'un ordinateur portable avec une *ransomware* de nos clients remonte à 2017. Dans ce cas, il a suffi d'isoler la machine et de recourir à des sauvegardes. » De manière générale, les sauvegardes et l'isolation des machines infectées sont d'après lui les principaux mécanismes utilisés lorsque la prévention et la détection ne suffisent pas.

Plan d'urgence

« En cas d'attaque coordonnée sur l'ensemble du secteur de la santé avec un impact significatif au niveau national, le Haut Commissariat à la sécurité nationale a élaboré le 'Plan d'intervention d'urgence Cyber (PIU Cyber)' pour faire face également à cette situation », explique Paul Rhein. Mais jusqu'à ce jour, cela n'a pas été nécessaire : « Jusqu'à présent, aucun des nombreux pirates n'a réussi à crypter des données chez nous ou à obtenir une rançon. »

Mais en dernière instance, souligne M. Rhein, la « responsabilité juridique incombe au 'propriétaire' du système informatique ». Et ces dernier·ère·s n'aiment pas que l'on s'immisce dans leurs affaires concernant la cybersécurité. Interrogé par le *Journal*, le Centre Hospitalier Emile Mayrisch (CHEM) a uniquement confirmé que ses équipes informatiques étaient conscientes des dangers et qu'elles surveillaient la situation en collaboration avec GOVCERT (point de contact central pour tous les types d'incidents informatiques pouvant mettre en danger les systèmes d'information du gouvernement et d'autres gestionnaires d'infrastructures publics ou privés considérés comme critiques). Selon le Chem, il est donc impossible d'en dire beaucoup plus pour des raisons de sécurité. Les autres hôpitaux n'ont pas souhaité faire de commentaires sur le sujet.

« La cybersécurité ne constitue jamais une tâche achevée », résume le directeur du GOVCERT, « mais un processus continu ». Des attaques de plus en plus fréquentes et sophistiquées ne faciliteront certainement pas ce processus à l'avenir, surtout si, dans les hôpitaux, chaque seconde et chaque lit disponible comptent déjà.

Publié le 02.12.2021
Mis à jour le 15 déc. 2021 à 20:33

Misch Pautsch

Journaliste et photojournaliste

Lex Kleren

Photojournaliste et rédacteur d'images